

January 14, 2002
Date

David R. Brown
Express Mail Label No.:
EL846223023US

- 1 -

KEY INFORMATION ISSUING DEVICE, WIRELESS OPERATION DEVICE,
AND PROGRAM

BACKGROUND OF THE INVENTION

5 The present invention relates to a key information processing technology.

10 Key information has hitherto been utilized in a variety of scenes in the human society. For example, data communications requiring the confidentiality of information involve using encryption keys. Further, what key information is recorded on magnetic stripes is used as a key for a building and an office as a substitute for a metallic key matching with a configuration of a key hole. Pieces of information on encryption keys and keys for the buildings etc are generically termed key
15 information.

20 The prior art system is, however, incapable of easily changing such a piece of key information and reissuing the key information. Alternatively, even if capable of reissuing the key information, a cipher is required to be stored, and hence the re-issuance needs a re-storing process, which is time-consuming. Therefore, though the encryption keys are used in the communications between information devices such as personal computer (which hereinafter be abbreviated to a PC) and so on, simple communications performed in daily life such
25 as communications between a TV receiver and a wireless remote controller thereof and communications between a wireless keyboard and the personal computer, do not involve the use of

the encryption keys.

Supposing that, for instance, home banking through the wireless remote controller and the wireless keyboard will be conducted from now on into the future, however, it is desirable that those communications be performed in an encryption-oriented system. It is because a password etc of a bank account might be intercepted (wiretapped).

It is required that a cipher be agreed upon between communication devices in order for communicating parties to decrypt such a cipher. Accordingly, there is needed a system capable of readily issuing the encryption key with security between the TV receiver and the wireless remote controller and between the PC and the wireless keyboard.

On the other hand, magnetic stripe type and IC card type keys (which will hereinafter be called electronic keys) used for locking and unlocking, e.g., a building, an office and so on, are convenient to carry and therefore easy to be lost and to become a target for theft. These types of keys are managed by, e.g., a center of a key (or building) management company.

Hence, if such a key is lost, all the keys distributed for using the building and offices must be collected, and the key information must be rewritten. The collection and re-issuance of the keys are very time-consuming.

SUMMARY OF THE INVENTION

It is a primary object of the present invention to provide a technology capable of easily issuing key information to a key

information retaining device that retains the key information.

It is another object of the present invention to provide a technology capable of ensuring sufficient security for protecting the key information when issued from being intercepted.

To accomplish the above objects, according to one aspect of the present invention, a key information issuing device (1, 1A, 1B) issuing key information to a key information retaining device (2, 2A, 2B), comprises an authentication module (14, 3) authenticating an issuer of the key information, an output module (13) outputting the key information to the key information retaining unit, and a recording module (11) recording a mapping of the issued key information to the key information retaining unit, wherein the key information is issued in response to an indication of the authenticated issuer.

Preferably, the key information retaining device (2, 2A, 2B) may be a wireless operation device (2, 2A) wirelessly connected to an information device and may include a key information input module (23) inputting the key information in contact with the key information issuing device, and the output module (13) may include a contact module outputting the key information in contact with the key information input module (23).

Preferably, the key information retaining device (2, 2A, 2B) may be a wireless operation device (2, 2A) wirelessly connected to an information device and may include a medium input module inputting information from a recording medium, and the output module (13) may include a recording medium write module

writing the information to the recording medium, and may issue the key information through the recording medium.

Preferably, the key information retaining device (2, 2A, 2B) may be a wireless operation device (2, 2A) wirelessly
5 connected to an information device and may include a near communication module incapable of performing communications beyond a predetermined distance, and the output module (13) may include a near communication module incapable of performing the communications with the key information retaining device beyond
10 a predetermined distance, and may issue the key information through the near communication module.

Preferably, the key information issuing device (1, 1A) may further comprise a receiving module (13) receiving wireless signals from the key information retaining device, and a decoding
15 module (11) decoding the information contained in the wireless signals and encrypted with the key information.

According to another aspect of the present invention, a wireless operation device (2, 2A) wirelessly connected to an information device, comprises a key information input module
20 (23) inputting key information for encrypting the information, a recording module (24) recording the key information, an operation module (22) detecting an operation of a user, an encryption module (21) encrypting user's operation based input information with the key information, and a transmission module
25 (25) transmitting the encrypted input information to the information device.

Preferably, the key information input module (23) may

include a contact module inputting the key information in a contact manner.

Preferably, the key information input module (23) may include a medium input module inputting information from a
5 recording medium.

Preferably, the key information input module (23) may include a near communication module incapable of performing communications beyond a predetermined distance.

Preferably, the wireless operation device (2, 2A) may
10 further comprise a setting module setting an execution or non-execution of the encryption, wherein the encryption module may encrypt the input information when the execution of the encryption is set.

According to still another of the present invention, a
15 wireless operation device (2, 2A) wirelessly connected to an information device, comprises an operation module (22) detecting a user's operation, a transmission module (25) transmitting user's operation based input information, and a confirmation module (21) confirming whether there is a response signal from
20 the information device with respect to the transmitted input information, wherein the transmission of the input information is stopped if the response signal is not obtained.

According to a further aspect of the present invention, a wireless operation device (2, 2A) wirelessly connected to an
25 information device, comprises an operation module (22) generating input information by detecting a user's operation, a simulated information generating module (21) generating

simulated information simulating the input information, and a transmission module (25) transmitting the input information or the simulated information.

Preferably, the simulated information may be transmitted
5 irrespective of whether the user's operation is made or not (S2A-S2C).

Preferably, the key information retaining device (2, 2A, 2B) may be an electronic key (2B) that unlocks a predetermined area.

10 According to a still further aspect of the present invention, a key information managing method of managing key information issued to a key information retaining device, comprises authenticating an issuer of the key information (S10-S11), generating key information (S15), outputting the key
15 information to the key information retaining unit (S16), and recording a mapping of the issued key information to the key information retaining unit (S1B).

According to a yet further aspect of the present invention, there is provided a program executed by a computer to actualize
20 any one of the functions described above.

According to an additional aspect of the present invention, there is provided a readable-by-computer recording medium recorded with such a program.

As described above, according to the present invention,
25 it is possible to ensure the sufficient security for protecting the communication between the information device and the wireless remote control from being intercepted. According to the present

invention, the key information can be easily issued to the key information retaining device for retaining the key information. Further, according to the present invention the sufficient security against the interception can be ensured when issuing the key information.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram showing an information system as a whole in a first embodiment of the present invention;

FIG. 2 is a block diagram showing a remote controller 2;

FIG. 3 is a diagram showing a data structure of a packet;

FIG. 4 is a flowchart showing steps of distributing an encryption key to the remote controller 2 from a main unit 1;

FIG. 5 is a flowchart showing a process when operating the remote controller;

FIG. 6 is a flowchart showing details of a process of encrypting button information;

FIG. 7 is a flowchart showing details of a process of sending a button information packet and a dummy packet;

FIG. 8 is a flowchart showing a process when in a receiving operation of the main unit 1;

FIG. 9 is a diagram showing a system architecture of an information system for executing home banking in a second embodiment of the present invention; and

FIG. 10 is a diagram showing a system architecture of an information system for executing a security management of an office in a third embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Preferred embodiments of the present invention will hereinafter be described with reference to the accompanying
5 drawings.

<<First Embodiment>>

A first embodiment of the present invention will hereinafter be described with reference to FIGS. 1 through 8. FIG. 1 is a diagram showing an information system as a whole
10 in the first embodiment. FIG. 2 is a block diagram showing a wireless remote controller 2. FIG. 3 is a diagram showing a data structure of a packet transmitted and received between a main unit 1 and the wireless remote controller 2. FIG. 4 is a flowchart showing steps of distributing an encryption key to
15 the wireless remote controller 2 from the main unit 1. FIGS. 5 through 7 are flowcharts each showing a process when operating the wireless remote controller 2. FIG. 8 is a flowchart showing a process when the main unit 1 receives the packet.

<Outline of Functions>

20 The information system in the first embodiment is operated through wireless communications by the remote controller. This information system authenticates a user and issues an encryption key for every remote controller operated by the user. At this time the information system records the encryption key issued
25 for every remote controller.

When the user operates the information system by the remote controller, input information is encrypted by the encryption

key. Then, the remote controller transmits a start-of-communication request to the information system and transmits the encrypted input information.

The information system identifies the remote controller in response to the start-of-communication request transmitted from the remote controller. Then, the information system collates the encryption key issued to the requester remote controller with the key among those recorded. Subsequently, the information system decodes the input information with this encryption key and detects an operation of the user.

The encryption key is distributed in the following steps.

(1) A device on the main unit of the information system executes authenticating the user identity. This process is to confirm whether the user is qualified for receiving a distribution of key information.

(2) Next, the main unit confirms proximity of the remote controller to the device itself.

(3) Subsequently, the main unit generates an encryption key (e.g., a random number).

(4) The main unit transmits the encryption key via a safety communication path that prevents an interception (wiretapping).

(5) The main unit confirms that the remote controller receives the encryption key in safety.

<Whole Architecture>

FIG. 1 is the diagram showing the whole architecture of the present information system. As shown in FIG. 1, this information system is configured by the main unit 1 and the

wireless remote controller 2.

The main unit 1 is categorized as an information processing device capable of communicating with an outside system via an unillustrated network. The main unit 1 may be, for example, a personal computer (which will hereinafter be abbreviated to PC), a digital TV, a set-top box and so on.

The main unit 1 includes a PC-equivalent function module 11, a remote controller proximity confirmation module 12, a remote controller communication module 13 and an authenticating function module 14.

The PC-equivalent function module 11 includes a CPU for providing an information processing function, a memory for storing the information and a communication interface for accessing the network. The architecture and operation thereof are nowadays broadly known, and hence their explanations are herein omitted. The PC-equivalent function module 11, based on this architecture, controls the main unit 1 and provides a variety of information processing functions.

For example, the PC-equivalent function module 11 generates the encryption key to be transmitted to the wireless remote controller. The generation of the encryption key involves generating a random number (or prime number) by a predetermined algorithm. The generated encryption key is required when in the remote communications and is therefore recorded and stored in the unillustrated memory of the main unit 1.

The PC-equivalent function module 11 embeds an ID for

identifying the wireless remote controller into this key. Then, the PC-equivalent function module 11 records a mapping table containing the IDs of the wireless remote controllers 2 and the encryption keys distributed.

5 The ID may involve the use of a production number (serial number) of the wireless remote controller 2. Further, the ID of the remote controller may also be generated by use a random number. With this ID, the present information system can administer a plurality of remote controllers. If one single
10 remote controller is to be used, the ID is not required. If there are other necessary pieces of information, these pieces of information may be contained in a part of the encryption key.

Further, the PC-equivalent function module 11 checks whether the wireless remote controller 2 surely receives the
15 encryption key. In this case, the PC-equivalent function module 11 can confirm it simply by, for instance, indicating the wireless remote controller 2 to transmit the encryption key back. Moreover, the wireless remote controller 2 may transmit only a checksum of the encryption key back to the module 11. Even
20 if failing to transmit the encryption key, the wireless remote controller 2 just falls into an unusable state and becomes usable by retrying the distribution steps. Accordingly, if the reliability of the encryption key transmission process is sufficiently high, there may be omitted the confirmation of
25 whether the wireless remote controller 2 surely receives the encryption key.

The PC-equivalent function module 11 provides a function

of authenticating the user identity. The authentication method includes a biometrics authentication using a fingerprint, sound spectrogram etc, a code number authentication, a password authentication and so forth. A method corresponding to a confidentiality required and an actualizing cost can be selected from those methods.

The authentication function module 14 checks based on the authentication method whether the user is qualified for indicating the distribution of the encryption key to the wireless remote controller 2. If the user is unqualified for indicating the distribution of the encryption key, the main unit 1 stops the process just when the user proves unqualified.

The remote controller proximity confirmation module 12 is, for instance, a push button and so on. The user, when making the wireless remote controller 2 proximal to the main unit 1, manipulates this remote controller proximity confirmation module 12 (e.g., presses the push button). With this manipulation, the main unit 1 recognizes the proximity of the wireless remote controller 2.

In this state, the main unit 1 performs wire communications or wireless communications using feeble radio waves with the wireless remote controller 2. The main unit 1 and the wireless remote controller 2 in such a state are illustrated in a lower part in FIG. 1.

The remote controller communication module 13 provides a function of transmitting the encryption key to the wireless remote controller 2. The remote controller communication

module 13 is configured of a communication interface and a communication program. Interfaces categorized as a serial system such as RS232C, a parallel system pursuant to the Centronics Standard and other wire systems are usable as the communication interface.

Thus, the present information system involves the use of the hard-to-intercept wire system for transmitting the encryption key separately from the wireless communication interface. Note that wireless communication interface is, for example, an infrared-ray receiving module, a wireless LAN interface and so on. The wireless communications may, however, also be utilized for transmitting the encryption key by using an electromagnetic shield in combination.

Further, a close range wireless system incapable of communications at a predetermined distance or farther may also be used. In this case, the remote controller communication module 13 may incorporate both of the encryption key transmitting function and a function of receiving an encrypted operation signal from the wireless remote controller 2.

In this case, an interception countermeasure such as reducing a transmission output when in close proximity, may be taken together with the electromagnetic shield. Note that there is no limit to a data format for distributing the key information described above.

FIG. 2 is the block diagram showing the wireless remote controller 2. The wireless remote controller 2 shown in FIG. 2 includes a processing unit 21 for controlling the components

of the wireless remote controller 2, a keyboard 22 for detecting a user's operation on the information system and generating input information, an encryption key receiving module 23 for receiving the encryption key from the main unit 1 of the information system, a memory 24 to and from which the processing unit 21 writes and read the information, a transmitting/receiving module 25 for transmitting and receiving the information in the wireless communications in accordance with an indication given from the processing unit 21, a display unit 26 for displaying various items of information, an encryption ON/OFF switch 27 for specifying whether the encryption is executed or not, and a power unit (battery) for supplying the electric power to the wireless remote controller 2.

The processing unit 21 is, for instance, a microprocessor. The processing unit 21 executes a control program loaded in the memory 24, thereby providing the function of the wireless remote controller 2. For example, the processing unit 21 receives the encryption key from the main unit 1 via the encryption key receiving module 23. Further, the processing unit 21 encrypts the information to be transmitted to the main unit by use of the encryption key received.

The keyboard 22 contains, in addition to alphabetic and numeral keys, a variety of buttons, an ON/OFF switch and so on. The user inputs an indication to the information system by manipulating these keys, buttons and switch.

The encryption key receiving module 23 is defined as a communication interface corresponding to the remote controller

communication module 13 of the main unit 1 described above.

The memory 24 is constructed of a random access memory (RAM) and a read-only memory (ROM). The memory 24 is stored with programs executed by the processing unit 21 and tables used
5 by the processing unit 21.

10 The transmitting/receiving module 25 is a communication interface for performing the wireless communications with the main unit 1. The transmitting/receiving module 25 is, e.g., an infrared-ray emitting module and an infrared-ray receiving

module, and a wireless LAN interface.
The display unit 26 displays an operation state of the wireless and so on. For example, the display unit 26 is a power lamp, etc.

15 The encryption On/Off switch 27 specifies whether the information is encrypted in the processing unit 21. This encryption On/Off switch is, provided so that the present wireless remote controller 2 is used for the general purpose, for an example, in a case that the information needs to be encrypted in the communications with a TV receiver etc and an operation
20 signal of an air-conditioner does not require the encryption (which means that a control unit of the air-conditioner is not adapted to the encryption). The user does an on/off setting of the encryption in accordance with a target operated by the wireless remote controller 2 by use of the encryption On/Off
25 switch 27.

<Data Structure>

FIG. 3 shows an example of the data structure of wireless

communication data (which will hereinafter be referred to as a packet) transferred and received between the main unit 1 and the wireless remote controller 2. As shown in FIG. 3, according to the present information system, a start-of-communication packet, a communication permission packet, a button information/dummy packet and an acknowledgement packet are prepared as packets of this category.

The start-of-communication packet is used for the wireless remote controller 2 to request the main unit 1 to start the communications. As shown in FIG. 3, the start-of-communication packet has fields stored with a header, a packet ID, a remote controller ID, a piece of dummy data and a checksum.

The header is defined as a bit string that indicates the packet transferred and received between the main unit 1 and the wireless remote controller 2 in the present information system. Referring to FIG. 3, a bit string "55AA" (hexadecimal number) is exemplified as the header.

The packet ID is an identification number specifying a category of the packet. Referring again to FIG. 3, the ID "0000" is specified in the start-of-communication packet.

The dummy data in the start-of-communication packet is defined as a bit string embedded in an unused field of the start-of-communication packet. Further, the checksum is defined as a piece of information for confirming a validity of the data when receiving the packet.

The communication permission packet is a packet used for the main unit 1 to notify the wireless remote controller 2 of

a communication permission in response to the start-of-communication packet sent from the wireless remote controller 2. As shown in FIG. 3, the communication permission packet has fields stored with a header, a packet ID, a remote controller ID, a session ID, a piece of dummy data and a checksum.

The header, the packet ID, the remote controller ID, the dummy data and the checksum among these pieces of data are the same as those in the start-of-communication packet. Further, the main unit 1 notifies the wireless remote controller 2 of the session ID each time the communication permission or receipt acknowledgement is made. The wireless remote controller 2 encrypts the input information with the received key information and this session ID.

The button information/dummy data packet is categorized into a button information packet and a dummy packet. The button information packet is used for the wireless remote controller 2 to transmit the button information (input information of the button manipulated by the user) to the main unit 1. Further, the dummy packet is used for transmitting the dummy data.

As shown in FIG. 3, the button information/dummy packet has fields stored with a header, a packet ID, a remote controller ID, encrypted button information or dummy data and a checksum.

The encrypted button information among these pieces of data is a piece of input information generated when the user operates the wireless remote controller 2. The button information is previously encrypted with the encryption key and the session ID that have been transmitted from the main unit

1 to the wireless remote controller 2. Moreover, the dummy packet is a packet for preventing a third party from intercepting (wiretapping) the button information packet. The dummy packet contains dummy data simulating the button information. An
5 unspecified number of dummy packets are transmitted before and after the button information packet.

The acknowledgement packet is a packet used for the main unit 1 to notify the wireless remote controller 2 of an acknowledgement in response to the button information/dummy
10 packet sent from the wireless remote controller 2. As shown in FIG. 3, the acknowledgement packet has fields stored with a header, a packet ID, a remote controller ID, a "checksum of the received packet", a next session ID, and a checksum.

The "checksum of the received packet" among those pieces
15 of data is a checksum of the packet received at the previous session. Further, the next session ID is used for encrypting the button information next time.

<Operation>

FIG. 4 is the flowchart showing an example of an encryption
20 key distributing process. This process is a process of the program executed by the main unit 1 (the PC-equivalent function module 11) when the main unit 1 transmits the encryption key to the wireless remote controller 2.

In this process, the main unit 1 at first executes
25 authenticating the user's identity (S10). The authentication of the user's identity involves reading the remote controller ID, reading the authentication information from the user and

confirming the authentication information. The authentication information given from the user includes a fingerprint, a sound spectrogram, a code number or a password.

Next, the main unit 1 judges based on a result of this authentication whether the user is qualified for receiving the distribution of the encryption key (S11). This judgment is made based on a comparison between the given authentication information and the authentication information registered in the main unit 1. The main unit 1, when judging that the user is unqualified and is therefore unauthorized user, aborts the process.

Whereas if judging that the user is qualified, the main unit 1 next waits for the wireless remote controller 1 to approach the main unit 1 itself (S12). Then, the main unit 1 judges whether the wireless remote controller is in close proximity to the main unit 1 itself (S13).

Then, if the wireless remote controller 2 is not in close proximity, the main unit 1 judges whether it is a time-out or not (S14). If not the time-out, the main unit 1 returns the control to S12. Whereas if it is the time-out, the main unit aborts the process.

When judging in S13 that the wireless remote controller 2 gets approached, the main unit 1 generates the encryption key (S15). Next, the main unit 1 transmits the encryption key to the wireless remote controller 2 (S16).

Subsequently, the main unit 1 waits for a response from the wireless remote controller (S17). If there is no response,

the main unit 1 judges whether it is the time-out (S19). Then, if not the time-out, the main unit 1 returns the control to S17. Whereas if it is the time-out, the main unit 1 aborts the process.

When judging in S18 that there is the response, the main unit 1 judges whether this response is normal (S1A). If not normal, the main unit 1 returns the control S12, and repeats the same process.

When judging in S1A that the response is normal, the main unit 1 creates and updates a mapping table stored with the remote controller ID and the encryption key (S1B). Thereafter, the main unit 1 finishes the process.

FIG. 5 shows the flowchart shoring the operation of the wireless remote controller. This process is a process of the program executed by the processing unit 21 of the wireless remote controller 2. An execution of this process is triggered by power-on of the wireless remote controller 2 or by pressing an unillustrated reset button.

In this process, to start with, the wireless remote controller 2 initializes the wireless remote controller 2 itself and comes to a status of waiting for the encryption key (S20). Next, the wireless remote controller 2 judges whether the receipt of the encryption key is completed (S21).

When the receipt of the encryption key is completed, the wireless remote controller 2 saves the received encryption key together with its own remote controller ID, and sends a completion-of-receipt response (S22). Thereafter, the wireless remote controller 2 comes to a waiting status (S23).

This waiting status continues till a new encryption key is transmitted or a user's button manipulation is detected.

Namely, when the receipt of the encryption key is started, the wireless remote controller 2 returns the control to S21, and confirms the completion of the receipt. On the other hand, when detecting the user's button manipulation, the wireless remote controller 2 sends the start-of-communication packet (S24).

Then, the wireless remote controller 2 waits for the communication permission packet (S25). Subsequently, if unable to receive the communication permission packet from the main unit 1 in wait for a predetermined time, the wireless remote controller 2 shifts to the waiting status (S23).

While on the other hand, when receiving the communication permission packet, the wireless remote controller 2 executes encrypting the button information (S27). Namely, the wireless remote controller 2 encrypts the input information generated by the user's button manipulation.

Next, the wireless remote controller 2 sends a dummy packet (S28). The number of times with which the dummy packet is sent is unspecified (random).

Next, the wireless remote controller 2 sends a button information packet (S29). Next, the wireless remote controller 2 sends a dummy packet (S2A). The number of times with which the dummy packet is sent is too unspecified (random).

Next, the wireless remote controller 2 judges whether the button is manipulated (S2B). Further, if manipulated, the

wireless remote controller 2 returns the control to S27.

Whereas if not manipulated, the wireless remote controller 2 judges whether it is a time-out or not (S2C). If not the time-out, the wireless remote controller 2 returns the control to S2A.

5 With this process, the dummy packet is transmitted an unspecified number of times till it comes to the time-out even when the user does not operate the wireless remote controller 2. Whereas if it is the time-out, the wireless remote controller 2 shifts to the waiting status (S23).

10 FIG. 6 shows a detailed process of encrypting the button information (S27 in FIG. 5). In this process, the wireless remote controller 2, to begin with, judges whether the encryption On/Off switch 27 is switched ON (S270).

15 If the encryption On/Off switch 27 is switched OFF, the wireless remote controller 2 finishes the button information encryption process. Whereas if the encryption On/Off switch 27 is switched ON, the wireless remote controller 2 reads the key information (S271).

20 Next, the wireless remote controller 2 reads the session ID (S272). This session ID is obtained from the communication permission packet or the acknowledgement packet (see FIG. 3).

25 Next, the wireless remote controller 2 encrypts the input information with the key information and the session ID (S273). Thereafter, the wireless remote controller 2 finishes the button information encryption process.

FIG. 7 shows details of the process of sending the button information packet and the dummy packet (S28, S29 or S2A)

In this process, the wireless remote controller 2 at first sends the packet (the button information packet or the dummy packet) (S41).

Next, the wireless remote controller 2 waits for the acknowledgement packet (S42). Then, the wireless remote controller 2 judges whether the acknowledgement packet is received (S43). If the acknowledgement packet is received, the wireless remote controller 2 advances the control to the next process.

While on the other hand, when judging in S43 that the acknowledgement packet is not yet received, the wireless remote controller 2 judges whether it is a time-out (S44). If not the time-out, the wireless remote controller 2 returns the control to S42 (S44). If not the time-out, the wireless remote controller 2 returns the control to S42. Whereas if judging in S44 that it is the time-out, the wireless remote controller 2 shifts to the waiting status.

FIG. 8 is the flowchart showing a receiving operation of the main unit 1. Upon a start of this process, the main unit 1 comes to a status of waiting for receiving the start-of-communication packet (S30). Then, the main unit 1 judges whether the receipt of the start-of-communication packet is completed (S31).

Then, when the receipt of the start-of-communication packet is completed, the wireless remote controller 2 collates the received remote controller ID (simply written as ID in FIG. 6) with the mapping table (created and updated in S1B in FIG.

4) (S32).

Next, the main unit 1 judges whether the received remote controller ID is valid (S33). If judged to be invalid, the main unit 1 returns the control to S30.

5 Whereas if valid, the main unit 1 sends the communication permission packet (S34). Next, the main unit 1 comes to a status of waiting for the button information/dummy packet. Then, the main unit 1 judges whether the receipt of the button information/dummy packet is completed (S36).

10 The main unit 1, when the receipt of the button information/dummy packet is completed, sends the acknowledgement packet and further executes a decoding process (S37).

15 Subsequently, the main unit 1 judges whether the received packet is a dummy packet (S38). If judged to be the dummy packet, the main unit 1 returns the control to S35.

 If not the dummy packet, the main unit 1 takes in the button information (S39). Thereafter, the main unit 1 returns the control to S35.

20 <Effects of Embodiment>

 As discussed above, according to the information system in the first embodiment, the button information generated when operating the wireless remote controller 2 with respect to the main unit 1 or the information system, is encrypted. It is
25 therefore feasible to decrease the possibility in which the operation signal generated when the information system is operated through the wireless remote controller 2 might be

intercepted by the third party.

Further, on such an occasion, according to the present information system, the main unit 1 distributes the encryption key to the wireless remote controller 2 in the wire communications in a way that brings the wireless remote controller 2 into contact with the main unit 1 or the wireless communications using the feeble radio waves with the wireless remote controller 2 disposed in close proximity to the main unit 1. Hence, it is possible to reduce such a risk that the encryption key itself might be intercepted (wiretapped) by the third party.

Moreover, according to the information system in the first embodiment, the information communications are carried out in a predetermined shake-hand procedure, for instance, as by the start-of-communication packet and the response packet responding thereto. It is therefore possible to reduce the risk that the operation signal generated when operating the information system through the wireless remote controller might be intercepted by the third party.

Further, according to the information system in the first embodiment, for example, the dummy packets are transmitted before and after transmitting the button information packet. Hence, it is feasible to decrease the risk that the operation signal generated when operating the information system through the wireless remote controller 2 might be intercepted by the third party.

<Modified Example>

According to the first embodiment discussed above, the

main unit 1 and the wireless remote controller 2 communicate with each other by use of the packets as shown in FIG. 3. The embodiment of the present invention is not, however, limited to the architecture and steps described above. For example, the start-of-communication packet basically capable of transferring (containing) the remote control ID may suffice, and the header, the packet ID etc may be or may not be added as the necessity arises.

Moreover, a data size of the packet may be a fixed length or a variable length. In the case of the fixed length, the length may be adjusted by using the dummy data shown in FIG. 3.

In the embodiment discussed above, the key information is passed to the encryption key receiving module 23 of the wireless remote controller 2 in the communications from remote controller communication module 13 of the main unit 1 to the wireless remote controller 2. The embodiment of the present invention is not, however, limited to this architecture. The key information may be passed to the wireless remote controller 2 from the main unit 1 through a readable-by-computer recording medium such as a flash memory card and so on.

In this case, the writing portion (e.g., a card slot) to the recording medium may be provided in the main unit 1. Further, the wireless remote controller 2 may be provided with a reading portion (e.g., the card slot) from the recording medium.

Configurations of these accessing devices to the recording medium are broadly known, and hence their explanations are herein omitted.

In the embodiment discussed above, the input information is encrypted with the encryption key and the session ID. The embodiment of the present invention is not, however, confined to this method. For instance, the input information may be encrypted with only the encryption key without using the session ID.

Moreover, it is considered that all appliances in home are controlled by one single remote controller. In the case of utilizing the remote controller incorporating the encrypting function, On/Off states of the air-conditioners, the channels of the TV and operations of a personal computer are all encrypted.

For an example, the On/Off signals of the air-conditioner among these operations do not need the encryption, and there might be a case where it is difficult to provide the air-conditioner with the encrypting/decrypting function. In such a case, the remote controller may make an option of the encryption or non-encryption according to the necessity and may thus perform the communications. In this case, the encryption On/Off switch 27 shown in FIG. 2 may be set OFF.

Alternatively, the PC is entrusted with all the remote controller communications and may decode by totally using the encrypted communications. In this case, if there is not the PC, the appliance cannot be controlled, and the remote controller is unusable. Accordingly, it follows that a range of utilizing such a system is limited.

<<Second Embodiment>>

A second embodiment of the present invention will

hereinafter be described referring to FIG. 9. FIG. 9 is a diagram showing a system architecture of an information system for executing home banking in the second embodiment.

The discussion in the first embodiment has been focused on the architecture and the operation of the information system including the wireless remote controller 2 having the encrypting function and the main unit 1 operated by the wireless remote controller 2. The second embodiment will exemplify a case where this information system is applied to home banking. Other configurations and operations in the second embodiment are the same as those in the first embodiment. Such being the case, the same components are marked with the same numerals, and their repetitive explanations are omitted. Further, the reference to the drawings in FIGS. 1 through 8 will be made as the necessity may arise.

This information system is configured by a PC 1A implementing a remote controller function (which will hereinafter be abbreviated to the RC function), a remote controller 2A provided with a keyboard for operating the PC 1A, and a bank host computer connected to the PC 1A via LAN (Local Area Network)/WAN (Wide Area Network).

The configuration and the operation of the PC 1A with the RC function are the same as those of the main unit 1 in the first embodiment. Further, the configuration and the operation of the remote controller 2A with the keyboard are the same as those of the wireless remote controller 2 in the first embodiment.

The user inputs a code number to the PC 1A with the RC

function through the remote controller 2A with the keyboard in the home banking. The communication from the remote controller 2A with the keyboard to the PC 1A with the RC function is similarly encrypted as in the information system according to the first embodiment. This architecture is capable of reducing the possibility in which the code number etc is intercepted (wiretapped) by the third party when utilizing the home banking.

Note that the security in the communication from the PC 1A with the RC function via the LAN/WAN to the bank host computer has hitherto been ensured by the variety of methods.

Accordingly, the PC 1A with the RC function and the remote controller 2A with the keyboard in the second embodiment cover an area that has hitherto been considered to be lowest in security in the home banking.

<Modified Example>

The second embodiment discussed above has exemplified the case where the keyboard-attached remote controller 2A incorporating the encrypting function is applied to the home banking. The embodiment of the present invention is not, however, limited to this applied example. Namely, the remote controller 2A with the keyboard and the wireless remote controller with the encrypting function shown in the first embodiment, can be applied to various categories of information systems.

For example, the system described above can be applied when connected to an Internet provider. This is because the a password when connected to the Internet provider can be used in the same way as a credit card. The system for the encryption

on the network and on the telephone line is getting sophisticated, and hence an area exhibiting the lowest confidentiality may be the remote controller as viewed from the whole system. Accordingly, the wireless remote controller 2 enhances such a lowest-security area, i.e., enhances essentially the security of the system on the whole.

<<Third Embodiment>>

A third embodiment of the present invention will be explained with reference to FIG. 10. FIG. 10 is a diagram showing a system architecture of an information system for executing a security management in an office according to the third embodiment.

This system is configured by a key information management PC 1B for issuing an electronic key 2B used for an office worker to enter the room, an authentication information input device 3 for authenticating an issuer of the key information, a lock management device at an entrance of the building, a lock management device at a door of the office, and a key information communication path that connects these lock management devices to the key information management PC 1B.

A configuration of the key information management PC 1B is the same as that of the main unit 1 in the first embodiment. According to the third embodiment, the key information management PC 1B has a key information management table for managing the issued key information for every electronic key 2B of the key receiver. This key information management table is a mapping of IDs of the electronic keys 2B to the issued key information.

The authentication information input device 3 serves to authenticate whether the issuer issuing the key information is valid. This authentication information input device 3 is, for example, a fingerprint reader, a sound spectrogram analyzer, a keyboard for inputting a code number or a password, and so forth.

The electronic key 2B includes a memory for recording the key information. The electronic key 2B, for instance, a card formed with magnetic stripes, an IC card, or a stick recorded with magnetism- or IC-based information.

When the key information of the this electronic key 2B is inputted to the lock management device at the entrance of the building or at the door of the office, the key ID of the electronic key 2B and the key information are transmitted via the key information communication path to the key information management PC 1B. Then, if the key information management table has already been stored with the mapping of the key ID to the key information, the key information management PC 1B transmits an unlock command the lock management device, thereby unlocking the entrance or the door.

This electronic key 2B is distributed to the worker who unlocks the entrance of the building or the door of the office. Then, if the number of such new workers increases, the issuer of which the authentication information is registered issues the key information.

Namely, the issuer at first authenticates the issuer himself or herself by use of the authentication information input

device 3, and next commands the key information management PC 1B to issue the key information. The key information is thereby written to the new electronic key 2B. In this case, the ID of the electronic key 2B and the key information are entered in the key information management table.

Note that if the electronic key 2B is lost, the worker concerned notifies the issuer that the key 2B is lost. The issuer deletes the key information of the electronic key 2b distributed to that worker from the key information management table.

Further, the issuer input the key information a new electronic key 2B in the same procedures and transfers it to the worker concerned.

Thus, according to the system in the third embodiment, the authenticated issuer can simply issue the electronic key 2B.

Moreover, in case the electronic key 2B is lost, the lost electronic key 2B can be made ineffective without exerting any influence on other workers.

<<Readable-by-Computer Recording Medium>>

The program executed by the computer to actualize any one of the processes (functions) described above in the embodiments discussed above may be recorded on a readable-by-computer recording medium. Then, the computer reads and executes the program on this recording medium, thereby providing the function of the main unit 1, the PC 1A with the RC function, the encryption key issuing device 1B, the wireless remote controller 2, or the remote controller 2A with the keyboard shown in the embodiment discussed above.

Herein, the readable-by-computer recording medium embraces recording mediums capable of storing information such as data, programs, etc. electrically, magnetically, optically and mechanically or by chemical action, which can be all read
5 by the computer. What is demountable out of the computer among those recording mediums may be, e.g., a floppy disk, a magneto-optic disk, a CD-ROM, a CD-R/W, a DVD, a DAT, an 8mm tape, a memory card, etc..

Further, a hard disk, a ROM (Read Only Memory) and so on
10 are classified as fixed type recording mediums within the computer.

<<Data Communication Signal Embodied in Carrier Wave>>

Furthermore, the above program may be stored in the hard disk and the memory of the computer, and downloaded to other
15 computers via communication media. In this case, the program is transmitted as data communication signals embodied in carrier waves via the communication media. Then, the computer downloaded with this program can be made to provide the function of the main unit 1, the PC 1A with the RC function, the encryption
20 key issuing device 1B, the wireless remote controller 2, or the remote controller 2A with the keyboard.

Herein, the communication media may be any one of cable communication mediums such as metallic cables including a coaxial cable and a twisted pair cable, optical communication cables,
25 or wireless communication media such as satellite communications, ground wave wireless communications, etc.

Further, the carrier waves are electromagnetic waves for

modulating the data communication signals, or the light. The carrier waves may, however, be DC signals. In this case, the data communication signal takes a base band waveform with no carrier wave. Accordingly, the data communication signal embodied in the carrier wave may be any one of a modulated broadband signal and an unmodulated base band signal (corresponding to a case of setting a DC signal having a voltage of 0 as a carrier wave).

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
222